Testimony of Robert Douglas
Before the
Committee on Energy & Commerce
U.S. House of Representatives
--
Hearing on
"Phone Records for Sale:
Why Aren't Phone Records Safe from Pretexting?"
--
February 1, 2006

Chairman Barton, Ranking Member Dingell, members of the Committee, my name is Robert Douglas and I thank you for the opportunity to appear before the Committee to address the Committee's concerns about the theft of Americans' phone records.

I. Background and Basis of Knowledge

I am the CEO of PrivacyToday.com and work as an information security consultant to the private and public sectors on issues involving all aspects of identity theft, identity fraud, and customer information security. During the past nine years I have assisted the financial services industry, the general business community, government, and law enforcement agencies to better understand the scope and methodology of identity crimes through educational materials, presentations, auditing, and consultation.

My specialty is monitoring and investigating the practices of identity thieves, illicit information brokers, and illicit private investigators that use identity theft, fraud, deception, bribery, social engineering, and "pretext" to steal customer and proprietary records from a wide range of businesses. Additionally, I teach businesses, government agencies, and law enforcement how to detect and defend against these forms of theft in order to better protect all Americans.

This is my sixth appearance before the United States Congress to discuss information

security. Most relevant to today's hearing, I worked in 1998 with the House Financial Services Committee to expose the use of "pretext" and other forms of deceptive practices to steal and sell consumers private financial records maintained by financial institutions. That work resulted in the July 28, 1998 hearing titled "The Use of Deceptive Practices to Gain Access to Personal Financial Information". Testimony offered at that hearing resulted in the Gramm-Leach-Bliley Act provisions outlawing the use of deceptive practices to gain access to financial account information. In follow-up testimony I presented in a September 13, 2000 hearing before the same committee acting in its oversight capacity, I discussed the emerging and growing threat of deceptive practices being used to gain access to phone records--the precise issue before you today. [The 1998 & 2000 testimonies, along with my other congressional testimonies are available at PrivacyToday.com/speeches.htm]

Following the 2000 testimony I served as a consultant and expert to the Federal Trade Commission in the design and execution of Operation Detect Pretext, a sting operation to catch and civilly prosecute companies participating in the illicit information market.

In 2002 I testified as an expert witness on illicit information brokers and the role they play in identity theft and fraud before the Florida Statewide Grand Jury on Identity Theft.

From 2001 to 2004 I was an expert witness and consultant for the plaintiffs in Remsburg v. Docusearch, a suit brought by the parents of Amy Boyer against a private investigator selling illicitly obtained personal information via a web site. Ms. Boyer was murdered by an infatuated young man who purchased Ms. Boyer's social security number, date of birth, and place of employment from Docusearch who employed a

"pretexter" to impersonate an insurance company official to obtain the employment address of Ms. Boyer. Subsequently the killer gunned down Ms. Boyer as she left work.

I am currently serving as a consultant in a Pennsylvania murder case involving the sale by a private investigator of data-mining "research" about the victim to a deranged former employee who used the "research" to locate the victim and kill him.

I assisted Chris Hoofnagle of EPIC West, who deserves full credit for this issue reaching the attention of Congress, with the amended complaints submitted to the FCC & FTC by compiling the 40 companies named therein.

I have lectured before local, state, federal and international law enforcement, banking, and business associations on the topic of identity crimes.

I am the author of "Spotting and Avoiding Pretext Calls" which was distributed by the American Bankers Association to all member institutions. I am also the author of "Privacy and Customer Information Security – An Employee Awareness Guide", a training manual that has been used by numerous banks and businesses to train employees to defend against deceptive practices designed to steal customer information.

Prior to my work as an information security consultant I was a Washington DC private detective.

II. Identity Thieves Use the Same Methods

I'd ask the Committee to keep one important fact in mind while investigating the practices of illicit information brokers and illicit private investigators stealing phone and other consumer rerecords. The methods used by those industries are used by identity thieves and financial criminals every day in this country to defeat customer information security systems for a wide-range of businesses.

Additionally, in each case I've worked involving web-based illicit information providers, when we have been able to review the files of the company, there have been indications of identity thieves and other criminals – including stalkers – using those companies to buy information about Americans. Finally, as we are focusing on phone records today, I would hazard an educated opinion that one of the reasons that the FTC lists cell phone fraud as one of the most common forms of fraud resulting from identity theft is the ease with which cell phone records are stolen or purchased on the Internet.

For further background information, I recommend reading "Your Evil Twin", by Bob Sullivan. I'd also like to recommend Robert O'Harrow's "No Place To Hide" as an excellent work on the growing data-mining industry and a number of the public policy issues raised by this industry.

III. The Illicit Sale of Phone Records and Much More

News reports have served an important role in bringing the problem of web-based information brokers and private investigators selling detailed phone records to the attention of this committee, Congress, and the American people. While reporting by Robert O'Harrow of the Washington Post and Bob Sullivan of MSNBC on the sale of phone records dates back to the late 1990's, the issue has only recently caught the full attention of the American consumer and law enforcement agencies across the country.

In part this was due to the work of Frank Main at the Chicago Sun-Times who discovered that the Chicago Police were concerned that the sale of detailed cell phone records could jeopardize the safety of police officers and criminal investigations. Subsequently, Frank Main reported that the FBI was alarmed to learn in a test purchase of

a web-based information broker that anyone could obtain the cell phone records of a FBI agent within a matter of hours from placing the order.

As the committee will learn a bit later in my testimony, the Chicago Police and FBI were correct in their concerns as years ago the phone records of Los Angeles police officers had been sold by an information broker to organized crime.

But for the most part, the overwhelming number of news reports has inadvertently served to minimize the scope and extent of the problem. While the vast majority of reporting has focused on cell phone records and a small number of web-based brokers selling those records, the reality is that all entities that maintain consumer and proprietary information are under attack. The list includes, but is not limited to, telecommunication (including email and Internet service providers), cable and satellite television, utility (including electric, gas, water & sewer companies), and financial industries, plus all government agencies. In short, any business or government agency maintaining customer records or confidential proprietary information is at risk because identity thieves, illicit information brokers, illicit private investigators, corporate spies, and con artists know quite often the most effective tool for stealing highly valued information is the telephone.

In addition to minimizing the types of consumer information for sale, recent news reports have also inadvertently minimized the number of outlets and methodologies via which phone records can be purchased or stolen. Even the range of telecommunications records for sale has been inadvertently minimized with most media focusing on just the sale of cell phone records.

Specifically, there are far more web-based illicit information brokers and illicit private investigators than the 40 cited in the EPIC West complaint and there are a myriad of methods used to defeat phone company information security protocols far beyond the simple pretext of impersonating the customer. Additionally, when considering phone records, all types of telecommunications records are for sale—from home and business phone records to cell phone records to reverse-911 cell tower location information to pager records to GPS tracking devices to name just a few categories.

Finally, the reporting has inadvertently minimized the dangers posed by phone records and other forms of information stolen by means of pretext falling into the wrong hands when information brokers and private investigators sell either information obtained through pretext, or even database information, to individuals without any understanding of why the individual wants the information. Murders and assaults have occurred when information brokers and private investigators have not taken adequate steps to understand who they are providing information to.

With the caveat that <u>all</u> consumer records and government/business proprietary information are at risk; that there are far more than the 40 brokers and investigators selling phone and other records cited in the EPIC West complaint; and, that these records in the wrong hands have caused severe harm – including loss of life, I will confine the remainder of my testimony to the sale of phone records obtained most commonly through pretext and other forms of deception.

IV. To Understand Why Records Are Sold, You Need To Know Who Buys Them

To understand why the phone records of practically any American – from former presidential candidate General Wesley Clark to women hiding under threat of violence –

are for sale on the Internet, you need to know who is buying the bulk of the phone records that are obtained through illicit means. The overwhelming majority of phone records are purchased by attorneys, private investigators, skip tracers, debt collectors, and the news media.

Attorneys purchase the records as a means of discovery in all forms of litigation from divorce, to criminal defense, to "business intelligence". Private investigators buy phone records as a means of locating witnesses, developing leads, and developing evidence. Skip tracers use phone records to locate hard to find individuals who may be using deceit themselves to cover their tracks. Debt collectors find phone records a valuable tool in locating "deadbeats" who may be hiding from the collector and/or hiding assets. The news media – especially the tabloid press – want phone records to track celebrities' lives and develop leads in cases like the Jon Benet Ramsey murder, the Columbine massacre, and the freeway slaying of Bill Cosby's son. Each of these categories of users and purchasers have at one time or another made impassioned pleas to me that they need access to phone records – outside of normal judicial review processes – to conduct what they argue are socially beneficial services.

These buyers and their thirst for the information contained in detailed phone billing records resulted in the market and the cash flow that fed and encouraged the online sale of phone records. Specifically, the methods for stealing phone records had been known and in use for decades in order to service attorneys, private investigators, skip tracers, debt collectors, and the news media. With the advent of the Internet and the World Wide Web it was only a matter of time before some illicit information broker or private investigator decided to advertise the availability of phone records on the web. And once

the first ads appeared and other brokers and investigators learned how much money could be made selling phone records via the Internet – in some instances more than a million dollars per year for small operations – the feeding frenzy was on. So today there are hundreds of ads on the web (and in legal and investigative trade journals) for phone records and phone "research". And contrary to the language on those sites claiming to limit sales of personal information to attorneys; investigators; skip tracers; debt collectors; and, bail bondsmen, most of these companies will sell to anyone as long as they think you're not a reporter or law enforcement agency conducting a media expose or sting operation. Frankly, greed is the name of the game.

Those hundreds of ads on the web only represent the tip of the iceberg. Two other factors combine to push the total to thousands of outlets for purchasing phone records. First, many brokers and investigators don't advertise on the web or at all. These brokers and investigators work beneath the surface and develop clients by word of mouth while shunning publicity. Many of these hidden brokers and investigators are the actual sources – once removed – for the information sold via the web as many of the web-based operators are not skilled in the methods of stealing customer information and serve as mere front companies. Second, the brokers and investigators who shun a web presence but supply many of the web-based operations, also supply other brokers and investigators throughout the country who don't openly advertise on the web or anywhere else. And often those brokers and investigators service other brokers and investigators in a spider web or pebble-dropped-in-the-pond effect. Through this black market phone records may pass through several sources – at times including a bribed phone company insider – before reaching the eventual buyer. So in reality there are thousands of brokers and

investigators, on the web and off, comprising the totality of suppliers of illicit phone records. And the records are now for sale to anyone who wants them – regardless of reason.

V. How Phone Records Are Obtained

Phone records are obtained through numerous methods and sources. Some of these methods and sources have been publicly discussed – some have not.

By far the most common method is the use of "pretext". Pretext, used in this fashion, is the method of convincing someone you are a person or entity entitled to obtain the records sought. The term "pretext" when used in the context of obtaining confidential, statutorily protected, or consumer and proprietary information is actually a misnomer used by illicit brokers and investigators to add an air of legitimacy to the fraud they commit. The reality is pretext is a combination of identity theft and fraud. Identity theft because the individual carrying out the pretext needs to assume the identity of the rightful owner of the information sought – usually including biographical information such as name, address, social security number, and date of birth – in order to impersonate that individual during the pretext. Fraud because once impersonating that individual, the pretexter defrauds the rightful custodian of the information sought into turning the information over to an improper recipient.

To further understand pretext you need to know the code of the identity thief, broker, or investigator seeking information they don't have legitimate access to.

1) Know what piece of information you want.
2) Know who the custodian of the information is.
3) Know who the custodian will release the information to.

4) Know under what circumstances the custodian will release the information.

5) Become that person with those circumstances.

Once you know the code and apply a little imagination and bravado, you can steal almost any piece of information in this country.

But again, contrary to most reporting on this subject, the number of pretext methods and variations of those methods are vast and far beyond just merely impersonating the consumer. By way of example, in a state action brought under an unfair and deceptive trade practice statute captioned Massachusetts v. Peter Easton, Easton was caught calling into banks impersonating a federal banking official in order to get the banks to surrender consumer financial account records. In one of the current Verizon cases involving phone records, there is report indicating the information brokers were impersonating Verizon employees assisting disabled account holders. These are just two of literally dozens of variations of methods I am aware of that succeed thousands of times each day in defeating phone and other companies customer authentication procedures.

An important aspect in the conduct of a pretext is the ability of the illicit information broker or private investigator to purchase data about the individual consumer they seek to impersonate. After all, to fraudulently convince a customer call center representative that the pretexter is the actual customer, the pretexter needs to know the full name; social security number; date of birth; address; and, other forms of personal identifying information of the actual account holder. In order to gain access to this information, the illicit information brokers and private investigators need to have subscriber accounts with legitimate data-mining companies—also commonly referred to as information brokers.

Beginning approximately a year ago, it became more difficult for illicit information brokers and private investigators to get or maintain subscriber accounts with the large legitimate data-mining information brokers. This is because in the wake of reports of data breaches by legitimate information brokers and a wide variety of other businesses maintaining consumer records – coupled with congressional hearings examining the data breach problems and the ease with which personal information like social security numbers could be purchased from many of the illicit brokers and investigators we are discussing today – the legitimate data-mining information brokers began to curtail and in some cases terminate all sales of information to private investigators and other business lines with a history of improper resale or use of database information.

But other small and mid-size companies have stepped in to fill the void and continue to provide social security numbers and other personal identifiers to illicit information brokers and private investigators. I am aware of at least a dozen companies that illicit information brokers and illicit private investigators are using to obtain full social numbers and other biographical data in order to conduct pretexts against consumers and businesses. This is an issue crying out for attention by Congress.

The second most common method of gaining illicit access to phone records is bribery of a company employee or even the trade of information with inside employees working in skip-tracing and collection divisions within phone companies. There is a small but constantly present underground network of employees who trade information – sometimes lawfully, sometimes not – and those seeking information that have no lawful right to that information have learned how to tap those resources.

While I am not aware specifically of a case involving phone records where threats of violence were used to coerce phone company employees to supply information to criminals, that has happened in the financial services community resulting in federal banking regulatory agencies warning financial institutions of the trend a number of years ago. I would not be surprised if this was happening to phone company employees as well. Remember – information equals cash to all sorts of information thieves and they will do anything necessary to obtain the information they seek.

Finally, I have a substantial amount of evidence developed over nine years on methods, tactics, and sources used to obtain phone records that is inappropriate for revelation in an open hearing. I'd be happy to share this with the Committee, enforcement agencies, the phone associations, or companies in a closed setting.

VI. Phone Record Sales and "Spoofing" Services on the Web Are Most Alarming

While the totality of brokers and investigators selling phone records are troubling, the Internet-based operations are most alarming for the simple reason that by their very nature they allow a buyer to easily conceal their identity and intent in purchasing another citizen's records. This anonymity is a criminal's delight. From identity thieves to stalkers to child predators to corporate spies, the ability to conceal the identity and intent of the end user of the records is paramount.

Additionally, when consumers see the web sites advertising the sale of phone records and services like Caller-ID "spoofing" services designed to defeat Caller-ID, it increases mistrust between the consumer and businesses Americans provide information to, and increases the belief by many consumers that the government isn't protecting the American consumer.

Web based services like spooftel.com and the open sale of devices designed to show a different number on a Caller-ID system than the actual number the call is being placed from can be used as part of pretext and can even be used to defeat security systems for voicemail. In one well known demonstration of Caller-ID spoofing, convicted "hacker" Kevin Mitnick demonstrated for a reporter how he could make a call look like it was coming from the White House.

The use of spoofing services and devices as part of pretext is so well known within the investigative and information broker industries that advice on how to pick the best services is often bantered about. Here's an example:

> If you are considering using one of the numerous Caller ID Spoofing services, you may want to know several things before you sign-up.
>
> 1. Can this service be employed as part of your PI business, or is it just to be used for entertainment purposes?
> 2. If it is to be use only for entertainment purposes, do they offer a commercial version, and if so what are the differences?
> 3. Do they record/log all transactions?
> 4. Can you call 800 numbers, or other toll free line?
> 5. Can you call financial institutions through their web site, even if the financial institution is one you have an account with?
> 6. Can you use an anonymous Internet surfing software product (these change your IP number and make you appear as if you are accessing the internet from another state, country, etc.) to access their web site?
> 7. Will they inform you if they suspect fraudulent activity? What is their method for settling such a dispute?
> 8. Will they supply you with a list of all the activities that can lead to a cancellation of your account?

I raise the issue of Caller-ID spoofing fraud so this Committee will be aware that the extent of the problem is far more than just the sale of phone records. It is a myriad of techniques and use of technology designed to defeat information security systems. The use of these technologies – specifically Caller-ID spoofing devices and services should be outlawed immediately.

VII. Did The FTC Give Tacit Approval To The Sale Of Phone Records?

Given how prevalent and open the sale of phone records is, this Committee must be wondering how these companies and their devious practices have remained untouched by the Federal Trade Commission and other enforcement agencies. After all, the FTC is charged with stopping unfair and deceptive trade practices.

Congress and the American people have a right to ask a series of questions of the Federal Trade Commission when it comes to the sale of phone records. The questions include:

a) Was the FTC aware of the sale of phone records prior to recent news accounts?

b) If the FTC was aware, for how long has the FTC been aware?

c) Prior to recent media revelations and Congressional demands, did the FTC take aggressive steps to stop the sale of phone records?

d) Did the FTC signal tacit approval of the sale of phone records by private investigators?

e) Why has the FTC been AWOL when it comes to protecting phone records?

These questions are fair as, after all, the FTC is supposed to be the watch dog for the American consumer. Given my work with, study of, and access to information concerning the role of the FTC when it comes to illicit information brokers and private investigators I'd like to posit answers to the above questions as I believe the reality is that when it comes to phone records – and all other illicitly obtained consumer records – the watch-dog is nothing more than a lap-dog on a leash held by the illicit information brokers and private investigators.

a) Was the FTC Aware of the Sale of Phone Records Prior to Recent News Accounts?

Yes. The FTC has been aware of the sale of phone records due to the Touch Tone Information case; Operation Detect Pretext; the Boyer murder case; and direct interaction and communication with the private investigative profession – including direct inquiries from PI Magazine on the FTC's views regarding pretexting for phone records.

b) If the FTC Was Aware of the Sale of Phone Records, For How Long Has the FTC Been Aware?

The FTC has been aware of the problem since at least April of 1999 when the FTC filed an action against Touch Tone Information. While the FTC brought the action against Touch Tone for the sale of consumer financial information obtained by means of deception, the Touch Tone records available to FTC staffers were replete with thousands of instances of phone records being obtained and sold by means of deception.

In 2002 I interviewed the Colorado Bureau of Investigation detectives who broke the Touch Tone case and whose work the FTC piggy-backed in bringing the FTC complaint against Touch Tone. The detectives informed me the FTC showed little interest in following up on the voluminous records contained in the files of Touch Tone showing a vast network of hundreds of private investigators, attorneys, and media outlets around the country using Touch Tome to obtain phone and other records.

For example, as documented by the Washington Post, Touch Tone sold Kathleen Willey's phone records to a Montgomery County, Maryland private investigator during the investigation of President Clinton.

Additionally, the Touch Tone records contained the following letter listing phone and other records sold by James Rapp, co-owner of Touch Tone, about participants in the Jon Benet Ramsey murder investigation as reported by the Denver Post in a June 26, 1999 article titled, “Letter Details Information Rapp Dug Up”. Each reference to “tolls” means detailed phone records.

Here is the text of an undated letter purportedly written by James Rapp to a private investigator in California named Larry Olmstead, owner of Press Pass Media. Olmstead used Rapp to get information for his clients, primarily tabloid media outlets, prosecutors say.
Dear Larry,
Here is a list of all Ramsey cases we have been involved with during the past lifetime (sic).
1. Cellular toll records, both for John & Patsy.
2. Land line tolls for the Michigan and Boulder homes.
3. Tolls on the investigative firm.
4. Tolls and home location on the housekeeper, Mr. & Mrs. Mervin Pugh.
5. Credit card tolls on the following:
a. Mr. John Ramsey, AMX & VISA
b. Mr. John Ramsey Jr., AMX.
6. Home location of ex-wife in Georgia, we have number, address & tolls.
7. Banking investigation on Access Graphics, Mr. Ramsey's company, as well as banking information on Mr. Ramsey personal.
8. We have the name, address & number of Mr. Sawyer & Mr. Smith, who sold the pictures to the Golbe (sic), we also have tolls on their phone.
9. The investigative firm of H. Ellis Armstead, we achieved all their land and cellular lines, as well as cellular tolls, they were the investigative firm assisting the Boulder DA's office, as well as assisting the Ramseys.
10. Detective Bill Palmer, Boulder P.D., we achieved personal address and numbers.
11. The public relations individual "Pat Kroton" (sic) for the Ramseys, we achieved the hotel and call detail where he was staying during his assistance to the Ramseys. We also have his direct cellular phone records.
12. We also achieved the son's John Jr.'s SSN and DOB.
13. During all our credit card cases, we acquired all ticket numbers, flight numbers, dates of flights, departing times and arriving times.
14. Friend of the Ramseys, working with the city of Boulder, Mr. Jay Elowskay, we have his personal info.

But that was not all, nor was it the most alarming aspect of the sale of phone records contained in the Touch Tone case the FTC had access to. Through a conduit Touch Tone had sold phone and pager records of Los Angeles Police Officers to organized crime.

Again, the Denver Post reported on this shocking set of facts in a June 29, 1999 article titled, “Accusations against Rapps Widen, Pair Allegedly Sold Phone Numbers of L.A. Cops to Mobster”. Here is the text of the article:

> James Rapp, the Denver private detective charged with trafficking in confidential information about the Ramsey murder case, also furnished the private phone numbers of police officers to a member of the so-called "Israeli mafia," authorities say.
>
> Rapp allegedly got the unlisted home phone numbers and pager numbers for some Los Angeles police officers and funneled them through a middleman to Assaf Walknine, a reputed Israeli mafia member who'd been arrested on forgery charges, according to an affidavit unsealed Monday. Colorado Bureau of Investigation agent in charge Mark Wilson said the release of officers' numbers can be extremely dangerous.
>
> "Not only is it dangerous, but it definitely could compromise any investigation that could be ongoing," he said.
>
> Rapp and his wife, Regana, were indicted last week by the Jefferson County grand jury on two counts of racketeering, charges that carry maximum penalties of 24 years in prison and fines of $1 million on conviction.
>
> Authorities claim the Rapps ran a detective agency, Touch Tone Information Inc., that used subterfuge to obtain confidential information about the Jon Benet Ramsey murder investigation and passed it to the world tabloid media.
>
> The pair surrendered Monday. They were jailed, then released on bond of $25,000 for him and $10,000 for her.
>
> The CBI started investigating the Rapps in January after getting a referral from the Los Angeles Police Department, the affidavit says.
>
> The LAPD alleged that the Rapps helped get phone numbers of police officers for Walknine after Walknine's arrest in connection with an alleged scheme to forge credit cards and gold coins.
>
> Authorities believe that Walknine also "cloned" the pagers worn by the officers. For instance, every time L.A. Detective Mike Gervais would be paged, the person paging him would get a call from Walknine, the affidavit says.
>
> The middleman between Walknine and the Rapps was a former L.A. cop and convicted felon named Mike Edelstein, the affidavit says.
>
> "LAPD is most interested in Edelstein," CBI agent Bob Brown said. "He was buying the information for Walknine from (the Rapps). As I understand it, when Walknine was arrested, he admitted he got this information from Edelstein - the pager numbers, the home telephone numbers and home addresses of LAPD officers.

"At one point, Edelstein actually showed up at the front door of one of the police officers while the officer was at work and his wife answered the door," Brown said. "He gives his name and walks away. The officer believes Edelstein was stalking him or in some way trying to intimidate him."

Brown said Edelstein was a cop who was fired from the Los Angeles Police Department. Edelstein served a prison sentence for possession of an automatic weapon and, after getting out of prison, became a private investigator, Brown said. He later began using the Rapps and their Touch Tone Information Inc.

Brown said that Los Angeles police discovered Edelstein's connection with the Rapps after a Los Angeles shoplifter claimed he was a LAPD officer and showed them identification. It was a forgery and traced to Edelstein.

During a search of Edelstein's home, officers found a cover letter from Touch Tone Information Inc. with a price sheet stating that the company could obtain the address and phone tolls for any telephone in the United States or internationally. Touch Tone also claimed it could provide banking information on an individual or corporation.

A former employee of the Rapps told investigators that they excelled at obtaining confidential phone numbers and bank records.

The former employee said he overheard phone discussions between James Rapp and his clients, which led him to believe that Touch Tone clients were a mix of private investigators, lawyers and news reporters. [end of article]

c) <u>Prior to Recent Media Revelations and Congressional Demands, Did the FTC Take Aggressive Steps to Stop the Sale of Phone Records?</u>

The simple answer is no. Given the wealth of knowledge and intelligence coupled with client lists for hundreds of private investigators, attorneys, media outlets, and other buyers of phone records contained within the Touch Tone files - not to mention what the FTC learned in the Boyer murder case and Operation Detect Pretext - what did the FTC do to root out this market and stop the sale of phone records? Not a thing.

d) <u>Did the FTC Signal Tacit Approval of the Sale of Phone Records by Private Investigators?</u>

Arguably yes. In direct and indirect ways the FTC has signaled to the illicit brokers and investigators that the sale of phone records will be tolerated—as long as it isn't too blatant.

This happened indirectly by brokers and investigators noting the FTC was aware of the sale of phone records for years and had taken no actions against any individuals or companies selling the records. In places where investigators and brokers meet to discuss sources, tactics, methods, enforcement actions, and legislation, there has been a continuing dialogue for years that argues the practice of selling phone records must be OK since the FTC has done nothing about it.

Another indirect signal was sent to brokers and investigators as an unintended consequence of the passage of the anti-pretexting for financial information statute contained with the Gramm-Leach-Bliley Act. Brokers and investigators, rather than looking at the spirit of the law, interpreted the letter of the law to allow the continued use of pretext and other forms of deception to obtain consumer records other than financial records. And the FTC, in bringing the paltry number of cases it has to date under Gramm-Leach-Bliley and the Unfair and Deceptive Trade Practices Act, has inexplicably ignored the evidence in those cases of phone record sales. This did not go unnoticed by the illicit information brokers and private investigators and was again read as a green light to sell phone records.

In addition to indirect signals, the FTC, whether intending to or not, has directly signaled the brokers and investigators that phone record sales would be tolerated.

In January of 2005, the cover story of PI Magazine was "The FTC on Pretexting: The PI Magazine Interview with Joel Winston". The interview was conducted by PI Magazine Editor-in Chief, Jimmie Mesis. In the set-up to the interview Mesis describes the reason he interviewed Joel Winston as the following:

> "In an effort to get a definitive definition of pretexting and the potential risks and penalties for conducting pretexts, PI Magazine was granted an interview with Joel

> Winston, Associate Director of the FTC, Division of Financial Practices. His office has the responsibility to monitor and regulate the use of pretexting." [Emphasis added]

During the course of the interview which covered a number of aspects regarding the definition of pretexting; various pretexting tactics; Gramm-Leach-Bliley; Operation Detect Pretext; and, the Unfair & Deceptive Trade Practices Act, Mesis asked Winston about the use of pretext for phone records. The following Q & A resulted:

PI Magazine (PIM): Do you classify the acquisition of telephone toll records as a clear violation of deceptive business practices?
Winston: It's not what we traditionally look at as deception because you're deceiving party A, but party B is the actual party being harmed. But, we believe that, even though it has not been tested in the courts, that acquiring toll records through false statements constitutes deceptive business practices.

PIM: Is this an area the FTC is going to start looking into?
Winston: We are aware that there have been some concerns about that and were continuing to consider it.

Not exactly a clear and strong message from Mr. Winston, the FTC official charged with pretext regulation, that the sale of phone records will not be tolerated when Mr. Winston was afforded an ideal forum to send an unambiguous warning. And I would note that a year later when this issue exploded in the media, 6 months after the EPIC West complaint was filed with the FTC, the FTC still had not brought a single enforcement action against any company selling phone records.

The interview continued and in a later question Winston was asked:

PIM: Are there currently any FTC concerns about private investigators?
Winston: Not as a general matter. If I thought that there were major problems in the PI industry that concerned us, I would certainly tell you. As with any industry, there are occasional bad apples, but the PI industry as a whole is not an area about which we have any particular concerns… [Winston then discusses an area dealing with credit reports unrelated to pretext and phone records]

An objective reader—not to mention a subjective reader, like a broker or investigator, trying to read the tea leaves of Winston's answers—comes away with the distinct impression that the sale of phone records by brokers and investigators is not high on Joel Winston's or the FTC's priority list. Particularly when coupled with the fact that in the seven years that the FTC has been aware of the sale of these records, they hadn't brought a single enforcement action against a company selling phone records.

But don't take my word on how the investigators and brokers reading Mr. Winston's comments interpreted them. Instead, read how the interviewer, Jimmie Mesis, Editor-in-Chief of PI Magazine interpreted Mr. Winston's answers. In a statement to fellow investigators and brokers on July 11, 2005 titled EPIC FIGHTING PHONE RECORDS SALES, Mr. Mesis, responding to other investigators and brokers that were angered by the complaint EPIC West filed, stated:

([Bracketed comments and emphasis added by Douglas])

> Greetings,
> **There is no doubt that that one complaint to the FTC does not constitute "a problem"** . However, when that complaint comes from EPIC, we have a problem. This organization continues to exist by its consistent efforts to blast alleged violations of consumer privacy. **My immediate concern is not the FTC**, rather EPIC for their aggressive negative media publicity campaigns against PI's and their strong lobbying efforts in Washington, DC.
>
> **I recommend that you read my interview with the FTC and the specific comments about telephone records** at www.pimagazine.com/ftc_article.htm
> **The FTC wasn't too concerned about telephone information, but if PI's are going to blatantly advertise tolls directly to the public as a commodity, the FTC will get involved and we are going to lose that commodity and our ability to solve many cases because of it.**
> [**Note that Mesis considers Americans' phone records a "commodity"!**]
>
> PI's need to STOP promoting the selling toll records directly to the public as a commodity. Rather, use it as an investigative tool used in the course of your investigation to lead you to a missing person or to the lead you need to solve the case. **I also suggest that PI's promote such services as "telephone**

research" as compared to coming right out and mentioning tolls, non-pubs, etc.
[**Note that Mesis recommends hiding what is actually being sold on web sites by using terminology designed to deceive—this is a common practice within the trade and its web advertising**]

Roe and I decided last January to voluntarily remove our magazines from the books shelves at Barnes & Noble and many other book stores. We did this at a financial loss to make it a bit more difficult for the public to readily learn and see the suppliers of information that shouldn't be directly accessible to the public. We as professional investigators need to know who these sources are, yet we all need to do something to stop this avalanche of perceived identity theft hysteria that the media has latched onto.

Remember, one day....soon, you will no longer be able to get non-pubs, addresses for telephone numbers, and tolls, all because some new law is going to be passed. Why? Because PI's shouldn't be promoting these investigative tools as a commodity. Then, just like with GLB, a new law will eventually prevent us from using an amazing investigative resource that will be lost, and it won't be anyone's fault other than our own.

Please do you part,
Jimmie Mesis, Editor-in-Chief, PI Magazine, Inc.

So in Mr. Mesis' own words – again, this is the man who sat in the room and interviewed the FTC's Joel Winston – "There is no doubt that that one complaint to the FTC does not constitute "a problem"…My immediate concern is not the FTC… The FTC wasn't too concerned about telephone information…"

One wonders what additional off the record discussion may have taken place between Mr. Mesis and Mr. Winston that may have bolstered Mr. Mesis' belief that the FTC "wasn't too concerned about telephone information."

But the interview was a year ago and before the EPIC West complaint. Perhaps in light of the EPIC West complaint and resultant media attention to the issue, Mr. Winston of the FTC has had a change of heart - perhaps not.

In an article by Peter Svensson of the Associated Press published less than two weeks ago on January 18, 2006, Joel Winston again stated why he doesn't see the sale of phone records as an issue rising to the level of seriousness surrounding the sale of financial records.

In the context of the article, Winston stated:

> So why didn't the Touch Tone case put such businesses out of business?
>
> For one, the FTC went after Touch Tone not for snooping on the private lives of police officers but for "pretexting" financial information from banks.
>
> "Our primary focus there was on financial, because that's really where the most direct harm is," Joel Winston, associate director of the FTC's division of privacy and identity protection, said in an interview. "If I'm pretexting a bank and getting your bank account records I can drain your account."
>
> "With phone records ... not to minimize the intrusion on one's privacy, but generally it doesn't lead to any specific economic harm. It's a different kind of harm," Winston said. Nevertheless, he added, the practice "raises significant privacy concerns."

Perhaps Mr. Winston should sit down with police officers and their families and explain those responses. Perhaps Mr. Winston should sit down with the parents of murder victim Amy Boyer and explain those responses. Perhaps Mr. Winston should stop focusing on "economic harm" and start worrying about the lives at stake—and already lost—because of pretext for "non-economic" information. Perhaps it is time the FTC finds a replacement for Mr. Winston who, unlike Mr. Winston, understands the dangers inherent in the sale of phone records. Given Mr. Winston's inability to even analyze the information contained in the FTC's own case files—notably the Touch Tone case and Operation Detect Pretext —American consumers and this Congress should not

believe that the FTC, even if armed with a new law, will be aggressive in the protection of phone records area as long as Mr. Winston is in charge.

But as hard as it may be to believe, the problems at the FTC are more extensive than Mr. Winston. The problems are institutional. Even when the FTC has brought cases against individuals and firms using pretext to steal financial information, the result has been to signal the brokers and investigators selling such information that the odds of being caught are slim and that the FTC will not impose serious sanctions.

In the Touch Tone case the FTC trumpets that they fined Touch Tone $200,000. What the FTC is slower to point out is that they suspended the fine. So Touch Tone paid not one penny in fines. In Operation Detect Pretext 1,500 advertisements for the sale of personal financial information were located by the FTC. From that universe, only 3 firms were the subject of court action. And once again the FTC settled for minimal fines of $2,000 in two of the cases, and waived the fine in its entirety in the third case.

But perhaps the most brazen evidence of all that the FTC is viewed as a toothless, paper tiger is the case of FTC v. Information Search, Inc, and David Kacala. This is the third case of Operation Detect Pretext mentioned in the preceding paragraph where the FTC waived the fine entirely.

Not only is Information Search, Inc. still in business, until just a matter of days ago the web site, located at www.information-search.com was selling cell phone and other telecommunications records. And on a page named for the FTC, Information Search, Inc. has been publicly thumbing its nose at the FTC and Congress for what Information Search, Inc. views as the wrong-headed passage and enforcement of the Gramm-Leach-Bliley Act.

So for years, Information Search, Inc., having been once prosecuted by the FTC for selling financial records obtained through pretext, has continued to sell phone records with all the indicia that they too were obtained through deceptive means, and the FTC has not done a thing. I seriously doubt the FTC ever went back and looked at the information-search.com web site.

Only when increased media attention was brought to bear on the problem of the sale of phone records and EPIC West named Information Search, Inc. in its complaint, did Information Search, Inc. take down the web ads for phone records—hoping that by the time the FTC looked they wouldn't find the ads. But EPIC West's Hoofnagle was savvy enough to capture the offending pages and various search engines continue to have cached pages showing Information Search, Inc. offered cell and other phone records for sale.

Bottom line. The message that is repeated loud and clear throughout the investigative and broker industries on a regular basis is: No need to fear the FTC. Fear EPIC West. But just lay low. The media storm will subside. And the FTC will look the other way as usual.

In fact, let me quote a North Carolina licensed private investigator who just days ago had this to say about the publicity surrounding the availability of cell phone records and his prediction for how this will play out in Congress once lobbyists for the illicit information brokers and investigators go to work:

> Just my humble opinion, but the more we talk about this, and say things like what we are going to do, etc. the more we encourage people in general to use pay phones (if you can find one), office phone extensions, friends cell phones or friends home phones, etc. Lets stop this silly comments and discussions. The more "we stir it, the more it will stink." We keep shooting ourselves in the foot. Not to mention, the cost to obtain various "information" from various "brokers"

will only rise, putting some items of investigative value out of reach! Let it die, the Media will soon lose interest, and our lobbyists will stay on top of it in our interests in Washington, DC.

e) Why Has the FTC Been AWOL Ehen it Comes to Protecting Phone Records?

I wish I fully knew the answer to this question and it is one that this Committee and Congress should investigate. I do have definitive ideas about the problems at the FTC that I saw first hand when I served as a consultant to Operation Detect Pretext. I would be happy to share those observations and concerns with this Committee in a non-public setting if the FTC will release me from my non-disclosure agreement. All of my statements concerning Operation Detect Pretext in this testimony are based upon aspects of Operation Detect Pretext that the FTC has made public. But there is much more to the story that I am unable to discuss under threat of severe penalty given my signed agreement with the FTC which I will continue to honor.

VIII. The FTC's Attitude Towards Pretexting is Inexcusable

From an outsider's perspective it is very difficult to understand the lack of interest by the FTC when it comes to pursuing those who are using deception to obtain consumer records, including phone records. The FTC routinely goes after scams and fraud where there is a distinct element of buyer beware – in other words – the consumer using a little common sense could have avoided being scammed or defrauded. That's fine. Those types of con artists should be dealt with. Yet the FTC has shown great reluctance and reticence in stopping the theft of consumer records where the consumer has no way of knowing the records are being stolen and therefore cannot protect himself as the records are in the control of other corporate or government custodians. Given this fact – the theft

of consumer records cries out for assistance and prosecution by appropriate government agencies in order to defend the American consumer.

How many murders of Americans will it take before the FTC gets serious? How many law enforcement officers, their families, and investigations have to be put at risk before the FTC gets serious? What will this Congress and future Congresses do to exercise oversight and force the FTC to get serious?

IX. The Need For A Comprehensive Statute Protecting All Consumer Records

While it is important that this Committee and Congress move quickly to outlaw the sale of phone records, it is also time for this Committee and Congress to pass a broad anti-pretexting statute designed to outlaw the use of deception to steal any consumer record.

In 1998 I first testified before Congress to expose the use of pretext to steal financial information and that practice was outlawed in 1999. In 2000 I again testified before Congress warning that phone records had become the new record of choice for information brokers and private investigators to steal. Here we are six years later dealing with the consequences. If Congress does not move to outlaw the tactics used to steal information – instead of merely protecting categories of information in a piecemeal approach – I fear we will be meeting again and again to address category by category.

Already other categories of information are under attack. I have tape of an information broker recorded surreptitiously describing how he defeats cable and satellite television providers and public utility providers information security systems. In fact, many of the web-sites under scrutiny today advertise the sale of utility information and Post Office Box underlying street address information. Post Office Box information is

protected by regulation, but is commonly obtained by the filing of fraudulent forms stating that the requestor needs the underlying address information for service of process when that is not the case.

Bottom line. If Congress only moves to protect phone records, Congress will create a nightmare for another industry similar to what the phone companies are experiencing today.

Finally, Congress should consider making the use of deceptive practices to gain access to consumer information a criminal act with primary jurisdiction falling to the Department of Justice and F.B.I. while simultaneously empowering state attorney generals to act as well. As an aside, I would note that several state attorneys general have already begun prosecutions under their state unfair and deceptive trade practices acts within weeks of learning of the problem, while the FTC with knowledge of the phone records issue since 1999 has yet to bring an action. This is all the more reason that primary authority for enforcement should not be given to the FTC. To vest primary authority with the FTC acting in a civil capacity, given the agencies history of impotence, is to almost guarantee that the illicit practices will not stop.

X. Congress, Enforcement Agencies, and The Private Sector Must Work Together

Just passing legislation will not be enough. The enforcement and regulatory agencies must actively work to root out and prosecute those who are stealing information. Congress must exercise regular oversight of the enforcement agencies to keep the agencies focused on protecting the American consumer. And the phone companies, along with all consumer services companies, must use appropriate customer authentication protocols to protect their customers.

Following the 1998 hearings on the use of deceptive practices to steal financial information from financial institutions, the American Bankers Association moved aggressively to educate all member institutions about the theft of customer account information. Working together with the ABA, I authored several training documents that were provided free of charge by the ABA to member institutions. We conducted numerous telephone seminars and I appeared at dozens of ABA conferences all over the country to teach financial institutions about the threats posed by the practices of identity thieves, illicit information broker, and illicit private investigators. While it is still possible to find financial records for sale on the web, the number of offerings has been dramatically reduced through those efforts. I believe the phone companies – indeed all consumer services companies – working together with Congress, enforcement and regulatory agencies, and their representative associations can have similar success.

One final item for consideration. I have reluctantly come to the conclusion that it may be time for federal regulation of the private investigative trade. By this means minimum standards may be set to assist in weeding out those who have no regard for the law and are destroying the hard earned reputation of thousands of professional private investigators who serve in a vital capacity in out nation's justice system.

XI. Conclusion

Mr. Chairman, thank you for your invitation to appear before this Committee. I will do anything I can to be of assistance to the Committee, Congress as a whole, the enforcement agencies, the trade associations, or individual companies affected by these issues.